From: "Blair Taylor" <btaylor@memphistomorrow.org>
To: "Adams, Ben C." <badams@bakerdonelson.com>
"William Gibbons \(wgibbons\)" <wgibbons@memphis.edu>
Date: 1/27/2018 2:42:03 PM
Subject: keyless entry car hacking

This keyless entry hacking/car theft is a big deal! And upon some research this morning I found there are cheap/easy solutions --just keep your key fob in a what is known as a faraday bag which can be purchased at Walmart for $6.95. It doesn't have to be the freezer! https://mashable.com/2017/11/28/protect-your-car-wireless-relay-attack/#aIkaTkFHZgqG

We really need to find out from MPD and Sheriff what percentage of cars stolen (and of cars broken into) have been keyless entry to determine if this is a problem in Memphis – how would it not be?. The hacking devices are cheap (some as low as $22) and VERY easy to come by! https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/

https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/

UTHOR: ANDY GREENBERGANDY GREENBERG
ECURITY
3.21.16
0:33 AM

RADIO ATTACK LETS HACKERS STEAL 24 DIFFERENT CAR MODELS

FOR YEARS, CAR owners with keyless entry systems have reported thieves approaching their vehicles with mysterious devices and effortlessly opening them in seconds. After having his Prius burgled repeatedly outside his Los Angeles home, the New York Times' former tech columnist Nick Bilton came to the conclusion that the thieves must be amplifying the signal from the key fob in the house to trick his car's keyless entry system into thinking the key was in the thieves' hand. He eventually resorted to keeping his keys in the freezer.

Now a group of German vehicle security researchers has released new findings about the extent of that wireless key hack, and their work ought to convince hundreds of thousands of

drivers to keep their car keys next to their Pudding Pops. The Munich-based automobile club ADAC late last week made public a study it had performed on dozens of cars to test a radio "amplification attack" that silently extends the range of unwitting drivers' wireless key fobs to open cars and even start their ignitions, as first reported by the German business magazine WirtschaftsWoche. The ADAC researchers say that 24 different vehicles from 19 different manufacturers were all vulnerable, allowing them to not only reliably unlock the target vehicles but also immediately drive them away.

"This clear vulnerability in [wireless] keys facilitates the work of thieves immensely," reads a post in German about the researchers' findings on the ADAC website. "The radio connection between keys and car can easily be extended over several hundred meters, regardless of whether the original key is, for example, at home or in the pocket of the owner."

That car key hack is far from new: Swiss researchers published a paper detailing a similar amplification attack as early as 2011. But the ADAC researchers say they can perform the attack far more cheaply than those predecessors, spending just $225 on their attack device compared with the multi-thousand-dollar software-defined radios used in the Swiss researchers' study. They've also tested a larger array of vehicles and, unlike the earlier study, released the specific makes and models of which vehicles were susceptible to the attack; they believe that hundreds of thousands of vehicles in driveways and parking lots today remain open to the wireless theft method.

The Vulnerable Makes and Models

Here's the full list of vulnerable vehicles from their findings, which focused on European models: the Audi A3, A4 and A6, BMW's 730d, Citroen's DS4 CrossBack, Ford's Galaxy and Eco-Sport, Honda's HR-V, Hyundai's Santa Fe CRDi, KIA's Optima, Lexus's RX 450h, Mazda's CX-5, MINI's Clubman, Mitsubishi's Outlander, Nissan's Qashqai and Leaf, Opel's Ampera, Range Rover's Evoque, Renault's Traffic, Ssangyong's Tivoli XDi, Subaru's Levorg, Toyota's RAV4, and Volkswagen's Golf GTD and Touran 5T. Only the BMW i3 resisted the researchers' attack, though they were still able to start its ignition. And the researchers posit—but admit they didn't prove—that the same technique likely would work on other vehicles, including those more common in the United States, with some simple changes to the frequency of the equipment's radio communications.

The ADAC released a video that shows surveillance camera footage of a real-world theft that seemed to use the technique, as well as a demonstration by the group's own researchers.

How the Hack Works

The ADAC researchers pulled off the attack by building a pair of radio devices; one is meant to be held a few feet from the victim's car, while the other is placed near the victim's key fob. The first radio impersonates the car's key and pings the car's wireless entry system, triggering a signal from the vehicle that seeks a radio response from the key. Then that signal is relayed between the attackers' two radios as far as 300 feet, eliciting the correct

response from the key, which is then transmitted back to the car to complete the "handshake." The full attack uses only a few cheap chips, batteries, a radio transmitter, and an antenna, the ADAC researchers say, though they hesitated to reveal the full technical setup for fear of enabling thieves to more easily replicate their work. "We do not want to publish an exact wiring diagram, for this would enable even young [students] to copy the devices," says ADAC researcher Arnulf Thiemel. As it is, he says, the devices are simple enough that "every second semester electronic student should be able to build such devices without any further technical instruction."

The Wireless Key Problem

Most remarkable, perhaps, is that five years after the Swiss researchers' paper on the amplification attacks, so many models of car still remain vulnerable to the technique. When WIRED contacted the Alliance of Auto Manufacturers, an industry group whose members include both European and American carmakers, a spokesperson said that the group was looking into the ADAC research but declined to comment for now. The VDA, a German automakers' group, downplayed the ADAC's findings in response to an inquiry from WirtschaftsWoche, pointing to decreasing numbers of car thefts in Germany and writing that "action taken by the automobile manufacturers to improve the protection against theft were and are very effective."

None of that is particularly comforting to the many millions of drivers with wireless key fobs. In fact, vulnerabilities in these systems seem to be piling up faster than they're being fixed. Last year researchers revealed that they'd cracked the encryption used by the chipmaker Megamos in several different makes of luxury car owned by Volkswagen. And at the Defcon security conference, hacker Samy Kamkar unveiled a tiny device he calls "RollJam," which can be planted on a car to intercept and replay the "rolling codes" vehicle locking system manufacturers developed to stay ahead of earlier replay attacks.

The ADAC researchers warn that there's no easy fix for the attack they've demonstrated. Yes, car owners can use Bilton's solution and store their keys in a freezer or other "faraday cage" designed to block the transmission of unwanted radio signals. But ADAC researcher Thiemel warns that it's difficult to know just how much metal shielding is necessary to block all forms of the amplification attacks. Far better, he says, would be for manufacturers to build defenses into their wireless key fobs, such as timing constraints that could catch the long-range attacks. "It is the duty of the manufacturer to fix the problem," Thiemel says. "Keyless locking systems have to provide equal security [to] normal keys." Until then, plenty of cautious car owners will no doubt be keeping their own key fobs well chilled.

Blair Taylor
President
Memphis Tomorrow

22 North Front Street, Suite 670
Memphis, TN 38103
Office: 901.322.8080
btaylor@memphistomorrow.org

stt